ABSTRAK

Saat ini perkembangan teknologi mengalami kemajuan begitu pesat. Setiap perkembangan teknologi tersebut juga terdapat penyebaran informasi. Penyebaran informasi dapat dilakukan dengan sangat mudah dan sangat cepat. Tetapi, kerahasiaan informasi tersebut menjadi masalah yang cukup besar. Informasi tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab.

Sistem keamanan komputer menjadi sebuah hal yang sangat penting diperhatikan dalam masalah kerahasiaan informasi tersebut. Ilmu kriptografi sangat berguna dalam sistem keamanan komputer. Dari sekian banyak ilmu kriptografi, salah satunya adalah implementasi kriptografi pada level prototipe IC.

Pada penelitian ini dikembangkan prototipe sistem enkripsi dan dekripsi berbsis FPGA dengan menggunakan algoritma stream cipher Grain-128. *Input* yang digunakan pada penelitian ini berupa biner. Metode untuk membangun *stream cipher* yang digunakan adalah NFSR *(Non-Linear Feedback Shift Register)* dan LFSR *(Linear Feedback Shift Register)*. Menggunakan bahasa pemrograman Verilog *Hardware Description Language* (HDL) untuk mendeskripsikan fungsi rangkaian *digital.* Pengujian yang akan dilakukan pada penelitian ini adalah analisa proses enkripsi dan dekripsi, waktu proses enkripsi dan dekripsi, *avalanche effect*, *clock,* dan *area*.

Kata Kunci : Prototipe, Kriptografi, Grain-128, FPGA